PROCEDURE 1410.21
Issued: March 29, 2001
Effective Date: April 16, 2001

SUBJECT: Single Client Node
Virtual Private Network (VPN) (Single user VPN)

APPLICATION: Executive Branch Departments and sub-units and non-executive branch entities when accessing the State of Michigan (SOM) data communication networks and hosts from external public or not-trusted non-state-controlled networks using the Internet Protocol suite (TCP/IP).

PURPOSE: To standardize a single client node VPN (desktop or personal computer) security policy and guideline for State of Michigan agencies connecting to internal data communications networks from remote locations over networks not controlled, operated, or managed by or for the State of Michigan.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Strategic Policy

TELEPHONE: 517/373-7326
FAX: 517/335-2355

SUMMARY:

This procedure establishes IPSec as the single client VPN technology adhered to in compliance with the State of Michigan security policy and best practice to protect internal networks, devices, and hosts from external security threats posed by transmitting protected data over the Internet or other external network.

The IPSec framework provides personal computer or workstation authentication, integrity, confidentiality through encryption, and anti-replay security services. Personnel authentication will be achieved using enterprise approved two-factor authentication (currently Securid).

The applicable transport mechanisms and international standard protocols include:

TCP/IP

Applicable Internet Engineering Task Force Request for Comments include:

- RFC 2401 "Security Architectures for the Internet Protocol"
- RFC 2402 "IP Authentication Header"
- RFC 2403 "The use of HMAC-MD5-96 within ESP and AH"
- RFC 2405 "The ESP DES-CBC Cipher Algorithm with Explicit IV"
- RFC 2406 "IP Encapsulating Security Payload"
- RFC 2407 "The Internet IP Security Domain of Interpretation for ISAKMP"
- RFC 2408 "Internet Security Association and Key Management Protocol"
- RFC 2409 "The Internet Key Exchange"
- RFC 2410 "The NULL Encryption Algorithm and Its Use With IPSec."
- RFC 2411 "IP Security Document Roadmap"
- RFC 2412 "The OAKLEY Key Determination Protocol"

APPLICABLE FORMS: None.

PROCEDURES:

General Information:

The objectives of the ***single client node VPN standard*** are to:

Protect State of Michigan systems from unauthorized use.

Increase the level of security inherent in the State of Michigan network infrastructure.

Support the secure remote access needs of the State's agencies for its mobile, transient, and telecommuting workforce for 24 x 7 access to internal system hosted resources.

Prevent alteration, destruction, or modification of host information.

Prevent disclosure of protected information to unauthorized individuals.

Decrease the risk of disruption or interruption of network service levels.

Benefits expected:

Accommodate appropriate use of low-cost access to state resources over the Internet or business partner networks.

Increased security for internal hosts and networks.

Reduction of risks associated with use of Internet or Extra-net "public" networks.

Maintain acceptable levels of network management efficiency.

Accrue cost savings from use of public network connections when appropriate for mobile workers.

Easier maintenance and enforcement of enterprise level security policies.

Opportunity to integrate Quality of Service (QOS) practices.

Applicability:

Conditions of Application:

This standard applies to non-browser client connection from desktops, laptops, or workstations that require access to any internal State of Michigan host system, server, or network connected host, when the network, host, or device contains information that is classified as protected under Michigan compiled laws and the connection is carried over networks that are not managed by or specifically for the State of Michigan.

A client user VPN hosted by connection authorized under this standard will not be permitted to concurrently use the same VPN connection for general access to the Internet (No split tunneling enabled configurations are permitted on the client.). All routes redirected for the client user while attached as a VPN node to the enterprise concentrator will be directed and limited to internal hosts on the LMAN or SOM-WAN exclusively.

This standard applies to the Extranet client access. Extranet is defined as any State of Michigan to business partner Internet tunnel or direct connection or value added network connection, when one connecting client is outside of the State of Michigan's network and the internal destination host is on any of the State of Michigan's internal host networks.

This standard applies to Internet client access. Internet is defined as any State of Michigan employee, contractor, or partner connection across the public Internet, VPN tunneled, or Internet Service Provider access or through any Access Service Provider where one connecting client is outside of the State of Michigan trusted network perimeter and the internal destination host is on any of the State of Michigan's internal host networks.

This standard does not cover:

1. Client connections internal to the State of Michigan trusted perimeter networks (LMAN or SOM-WAN).

2. Secure Sockets Layer (SSL) enabled Web browser applications available to the Internet.

3. Intermittent connections made over the public switched telephone network using a plain old telephone (POTS) or integrated services digital network (ISDN) dial-in-connections to the State of Michigan's central modem bank. In cases where the client desktop is also connected to any shared media connection such as a cable modem or foreign local area network PROCEDURE 1410.20 is required to use the enterprise dial-in modem bank.

4. This standard does not address the total security access needs and is intended to supplement and/or be combined with other security standards and best practices when indicated as necessary to provide adequate risk reduction.

Assumption:

Agency remote users are accessing State of Michigan network and server resources with state agency provided equipment configured, managed, and maintained by agency technical staff. Where employees gain access to State of Michigan network and server resources with personal privately owned equipment, only SSL enabled web browser applications available to the Internet are employed for access. Further that these web browser enabled applications utilize application layer security best practices such as user name and password, and/or pin number combinations at a minimum, to reduce risk of unauthorized access leading to inappropriate use.

In addition to use of VPN technology to access protected data, agency network or host administrators shall provide appropriate security though best practices applicable to application level, network, or host security.

Implementation considerations:

This standard applies when the single client connections are for random intermittent periods of time.

Agencies must coordinate specific remote access needs with Telecom Operations-Network Operations Center (NOC) and review security risk threat profile analysis with the Enterprise Security Director.

DMB will deploy VPN Concentrators to provide IPSec enabled VPN clients on the Internet and/or Extranet connection points to State of Michigan networks. The concentrators will use hardware encryption. Issuance of shared-keys, establishment of access control lists, and access route lists for the Triple DES (3DES) Internet Key Exchange (IKE) negotiated encryption will require a written request to the Network Operations Center (NOC) from the agency security administrator. Pre-shared encryption keys when supported by the client operating system and the concentrator will require distribution of keys through the use an "out of band" method such as registered mail. The Network Operations Center and the agency security administrator will maintain chain-of-custody documents pertaining to shared-key issuance. Dynamic encryption key distribution will be done only in conjunction with Securid. Agencies shall establish internal procedures to promptly notify NOC when VPN privileges should be withdrawn from access control lists maintained by NOC. Revocation is at the agencies' discretion except when an employee is terminated or retires. Notification must be made to the NOC immediately when anyone in the chain-of-custody leaves State of Michigan employment.

Technical Considerations: The implementations of client node VPN will standardize on an L2TP/IPsec-enabled client with Windows 2000 desktop operating system configured for using a transport mode security association and digital encryption keys to provide 3DES encryption. Along with 3DES encryption the MD5 hashing algorithm will be used to provide data integrity. Non-repudiation or personal authentication when required for client connections will be provided by two-factor authentication currently provided by Securid cards. Issue of Securid cards are authorized by the agency security administrators signed letter to the Network Operation Center. All single-client node VPN connections will link to the enterprise concentrator before being routed thought the State of Michigan firewall and switched connections to internal networks.

In order to provide more management granularity, enhanced security, and access features, the concentrator's hardware-specific-client may be used. Use of the hardware-specific-client provides additional desktop operating system compatibility and management features. Under certain circumstances on the distant end such as where the Internet Service Providers are protecting their systems with firewalls or devices using network address translation (NAT) or private addressing schemes the use of the hardware-specific-client may be required or necessary to establish bi-directional communication.

Maintenance:

DMB: Acquisition Services shall not approve any acquisition or purchase request without confirmation from the Department of Information Technology, Office of Strategic Policy that such request is in compliance with the standard.

Operating Units (OU): Any and all projects, consulting requests, equipment and software acquisition requests, or ITB's relating to client, desktop, or personal firewall will be subject

to review for compliance with this standard.

DIT: The Office of Strategic Policy will review this standard on a continuing basis and make recommendations for changes. An appropriate group of staff, representing a wide-range of state operational units, will review and possibly revise these standards and guidelines as often as needed.

Exceptions from this standard for reasons other than those outlined above will be made through the exception handling process described in the Exception Process Template.

***